Varautuminen tiedonsiirtojärjestelmien ylläpitämiseen poikkeus-oloissa

Timo Kokko

Teknologiaosaamisen johtaminen koulutusohjelman opinnäytetyö

YAMK

KEMI 2013

ALKUSANAT

Haluan kiittää työni valmistumisesta ohjaajiani Jaakko Ettoa ja Sakari Seppästä. Lisäksi kiitän kaikkia läheisiäni, jotka ovat tukeneet minua opinnäytetyön tekemisen aikana.

Kiimingissä 20.2.2013

Timo Kokko

TIIVISTELMÄ

KEMI-TORNION AMMATTIKORKEAKOULU, Tekniikan ala

Koulutusohjelma:	Teknologiaosaamisen johtaminen
Opinnäytetyön tekijä(t):	Ins (AMK) Timo Kokko
Opinnäytetyön nimi:	Varautuminen tiedonsiirtojärjestelmien ylläpitämiseen poikkeusoloissa
Sivuja (joista liitesivuja):	48 (6)
Päiväys:	20.02.2013
Opinnäytetyön ohjaaja(t):	DI Jaakko Etto, Majuri Sakari Seppänen

Puolustusvoimien tulee normaaliolon aikana laatia suunnitelmia ja toimintamalleja, joilla pystytään mahdollisissa poikkeusoloissa ylläpitämään tiedonsiirtojärjestelmien toiminta. Tämän vuoksi varautuminen poikkeusoloja varten vaatii jatkuvaa yhteistyötä eri viranomaisten, tietoliikennepalveluita tuottavien teleoperaattoreiden sekä sähköyhtiöiden kanssa.

Tämän työn tavoitteena oli tarkastella niitä keskeisiä toimintoja, joiden avulla normaaliolotilan aikana voidaan parantaa kykyä ylläpitää tietoliikennejärjestelmiä poikkeusolojen aikaisessa tilanteessa. Tarkastelun ulkopuolelle jätettiin poikkeusolojen aikainen toiminta.

Tässä työssä käytettiin laadullista tutkimusmenetelmää, eli kvalitatiivista tutkimusta, jossa tutkimus suoritettiin dokumentaatioaineiston ja havaintojen perusteella. Jokaista erillistä tutkittavaa kohdetta arvioitiin tapauskohtaisesti.

Työn keskeisimpinä tuloksina laadittiin tarkistuslista, jonka avulla organisaatio pystyy tutkimaan omalla vastuualueellaan olevia viestiasemia ja löytämään niistä ne kohteet, jotka ovat palvelutuotannon kannalta tärkeimpiä. Tarkastelun pohjalta organisaatio pystyy laatimaan tarkempia toimintomalleja ja prosesseja, joiden avulla pystytään ennakoimaan ja estämään mahdolliset järjestelmien toimimattomuudet poikkeamatilanteissa ja poikkeusoloissa.

Henkilöstölle tehtävällä osaamiskartoituksella voitaisiin saada selville mahdollisia koulutustarpeita, joiden avulla osaamista organisaatiossa voitaisiin parantaa. Mikäli kartoituksessa selvästi havaitaan, ettei kouluttamisella saavuteta riittävää osaamista, voidaan ylemmälle taholle tehdä tarvittavia lisähenkilöstön rekrytointiesityksiä

Asiasanat: poikkeusolo, kunnossapito, riskianalyysi, tiedonsiirtojärjestelmä.

ABSTRACT

KEMI-TORNIO UNIVERSITY OF APPLIED SCIENCES, Technology

Degree programme:	Technology Competence Management
Author(s):	Timo Kokko, BEng
Thesis title:	Preparations of The Finnish Defence Forces to Maintain Communication Systems in Emergency Conditions
Pages (of which appendixes):	48 (6)
Date:	20 February 2013
Thesis instructor(s):	Jaakko Etto, MSc, Eng, Sakari Seppänen, Major

During normal conditions, The Finnish Defence Forces should make plans and operational models for maintaining communication systems during possible emergency conditions. This is why preparing to emergency conditions needs co-operation with different officials, teleoperators that produce telecommunication services and electricity companies.

The objective of this study was to view those essential functions that help to improve the ability to maintain communication systems during emergency conditions.

The study is based on a qualitative research method in which the research is carried out with the aid of documentary material and on the basis of perception. Each individual item is evaluated case by case.

The essential result of this study was the checklist, which the organisation can use to search all the communication stations in their area of responsibility and find targets in them that are the most important for producing the services. Based on the search, the organisation can make more precise operational models and processes that can be used to predict and prevent possible failure of the systems in emergency conditions.

The competence mapping done to the staff could clarify the training needs, which could improve the skills of the staff in the organization. If it is clearly noticed in the survey that the training does not produce enough expertise, it is possible to make the upper level of the organization propositions for recruitment of extra staff.

Keywords: emergency conditions, maintenance, risk analysis, communication system.

SISÄLLYS

KÄYTETYT MERKIT JA LYHENTEET

PVJJK	Puolustusvoimien Johtamisjärjestelmäkeskus
PSJJK	Pohjois Suomen Johtamisjärjestelmäkeskus
TUVE	Valtion Turvallisuusverkkohanke
SFS	Suomi Finland Standard
ITVJ	Integroitu tiedustelun, valvonnan ja johtamisen verkko
UPS	Uninterruptible Power Supply
DC	Direct current
AC	Alternating current
KATAKRI	Kansallisen turvallisuusauditointikriteeristö
EMP	Electromagnetic pulse
NEMP	Nuclear Electro-Magnetic Pulse
HEMP	High altitude ElectroMagneticPulse
LEMP	Lightning ElectroMagnetic Pulse
TEMPEST	Sähkömagneettinen hajasäteily

1 JOHDANTO

Tässä työssä tutkitaan Puolustusvoimien Johtamisjärjestelmäkeskukseen (PVJJK) kuuluvan Pohjois-Suomen Johtamisjärjestelmäkeskuksen (PSJJK) vastuualueella olevien tiedonsiirtoverkon rakentamis-, ylläpito- ja kunnossapitopalveluja. Tavoitteena on saada aikaan tiedonkeruumallit, joiden avulla voidaan etsiä palvelutuotannon kannalta tietoliikenneympäristöstä kriittisiä solmukohtia. Myös henkilöstölle mahdollisesti tehtävällä osaamiskartoituksella voitaisiin saada selville nykyinen osaamisen ja henkilöstöriittävyyden tilanne. Saatujen tietojen avulla voidaan jatkossa tehdä esityksiä ja suunnitelmia, joiden pohjalta kehitetään kunnossapidon organisaatiota ja henkilöstöä.

Tämän työn lähtökohtana on tietoliikenneverkoissa mahdollisesti esiintyvien häiriötilanteiden minimoiminen niin, että jo normaalioloissa voidaan järjestelmien toimivuus turvata mahdollisimman hyvin, eikä tarvitse tehdä erillisjärjestelyjä poikkeustilanteiden varalle. Häiriötilanteet saattavat syntyä laiteviasta, sähkökatkoksesta, materiaalin laatuvirheestä, suuronnettomuudesta, luonnonilmiöstä, käyttövirheestä, ilkivallasta, verkon operoijien tiedonpuutteesta tai näiden yhdistelmistä. Nämä häiriötilanteet voivat äkillisesti laajentua ja aiheuttaa tietoteknisille järjestelmille ennalta arvaamattomia ongelmatilanteita mikäli niihin ei ole varauduttu ja niiden riskiä ei ole tunnistettu.

Normaaliolossa häiriötilanteita varten suunnitellut ja rakennetut toiminta- ja ratkaisumallit ovat lähtökohtana ja perustana myös poikkeusolojen järjestelmien ylläpitämiselle. Näihin uhkiin varautuminen edellyttää niin viranomaisten, kuin eri yritysten ja laitetoimittajien sekä sähköyhtiöiden ja teleoperaattoreiden jatkuvaa yhteistyötä

Tässä työssä keskitytään tarkastelemaan Puolustusvoimien normaaliolojen toimintoja ja poikkeusolojen käsittely jätetään pois työn julkisuuden vuoksi. Poikkeusolojen osalta tutkimusta voidaan tehdä jatkotutkimuksissa, joissa tämä työ voi osin olla pohjatutkimuksena.

2 POIKKEUSOLOT JA MÄÄRITTELYT

Normaaliolojen häiriötilanteiden ja poikkeusolojen erottaminen toisistaan voi olla hankalaa ja näin ollen normaaliolojen häiriötilanteet voivat vaikutuksiltaan olla usein rinnastettavissa poikkeusoloihin. Nyky-yhteiskunnassa normaaliolojen uhkamallina on tilanne, jossa tekninen ja verkottunut yhteiskunta voi joutua häiriötilaan tiedonsiirtojärjestelmissä ilmenevien häiriöiden johdosta.

Poikkeusoloiksi ymmärretään yleensä sotilaallisten toimintojen aiheuttamat häiriöt, mutta riittävän isot uhat ja tapahtumat luokitellaan myös poikkeusoloiksi. Varautumisen tarkoituksen on laatia yritykselle politiikka, prosessit sekä toimintamallit joilla selvitään poikkeusoloista.

2.1 Poikkeusolo

Poikkeusoloja valmiuslain 1552 3 § mukaan ovat

1) Suomeen kohdistuva aseellinen tai siihen vakavuudeltaan rinnastettava hyökkäys ja sen välitön jälkitila;

2) Suomeen kohdistuva huomattava aseellisen tai siihen vakavuudeltaan rinnastettavan hyökkäyksen uhka, jonka vaikutusten torjuminen vaatii tämän lain mukaisten toimivaltuuksien välitöntä käyttöön ottamista;

3) väestön toimeentuloon tai maan talouselämän perusteisiin kohdistuva erityisen vakava tapahtuma tai uhka, jonka seurauksena yhteiskunnan toimivuudelle välttämättömät toiminnot olennaisesti vaarantuvat;

4) erityisen vakava suuronnettomuus ja sen välitön jälkitila;

5) vaikutuksiltaan erityisen vakavaa suuronnettomuutta vastaava hyvin laajalle levinnyt vaarallinen tartuntatauti.

Lain tarkoituksena on poikkeusoloissa suojata väestöä sekä turvata sen toimeentulo ja maan talouselämä, ylläpitää oikeusjärjestystä, perusoikeuksia ja ihmisoikeuksia sekä turvata valtakunnan alueellinen koskemattomuus ja itsenäisyys. (Valmiuslaki 1552/2011 1:3 §).

2.2 Varautuminen

Valtioneuvoston, valtion hallintoviranomaisten, valtion itsenäisten julkisoikeudellisten laitosten, muiden valtion viranomaisten ja valtion liikelaitosten sekä kuntien, kuntayhtymien ja muiden kuntien yhteenliittymien tulee jo normaaliolotilanteessa varautua toimimaan myös poikkeusoloissa. Vastaavat määritelmät pätevät myös erillisille teleyrityksille. Tämän vuoksi yritysten tuleekin jo normaalioloissa huomioida valmiussuunnitelmin ja poikkeusoloissa tapahtuvan toiminnan etukäteisvalmisteluin sekä testauksien avulla, sekä muilla toimenpiteillä varmistaa mahdollisimman hyvä toimiminen myös poikkeusoloissa. (Viestintämarkkinalaki 393/2003 9:90 §; Valmiuslaki 1552/2011 3:12 §).

2.3 Viestintäjärjestelmien toimivuuden turvaaminen

Poikkeusoloissa voidaan viestintämarkkinalain mukaiset teleyritykset velvoittaa viestintäjärjestelmien toimivuuden turvaamiseksi:

1) tuottamaan verkko- ja viestintäpalveluja, sekä antamaan viranomaiselle verkko- ja viestintäpalveluiden käyttöä koskevan tilannekuvan;
2) pitämään kunnossa tai rakentamaan, tai jättämään rakentamatta viestintäverkkoja;
3) luovuttamaan viranomaiselle tai toiselle teleyritykselle käyttöoikeuden viestintämarkkinalain 4 luvussa tarkoitettuun omaisuuteen; ministeriö voi myös päätöksellään kumota teleyritykselle viestintämarkkinalain nojalla asetetun käyttöoikeuden luovutusvelvollisuuden;
4) järjestämään kansainväliset verkko- ja viestintäpalveluyhteytensä liikenne- ja viestintäministeriön yksilöimällä tavalla;
5) sopimaan kansallisista tai kansainvälisistä verkkovierailuista liikenne- ja viestintäministeriön osoittamalla tavalla;
6) liittämään viestintäverkon yhteen toisen viestintäverkon kanssa tai purkamaan yhteenliittämisen;
7) katkaisemaan määräajaksi tai toistaiseksi verkko- tai viestintäpalveluyhteydet tiettyyn maahan tai kansainvälisiin verkko- ja viestintäpalveluihin;
8) ylläpitämään järjestelmiä ja palveluita tietyistä paikoista.

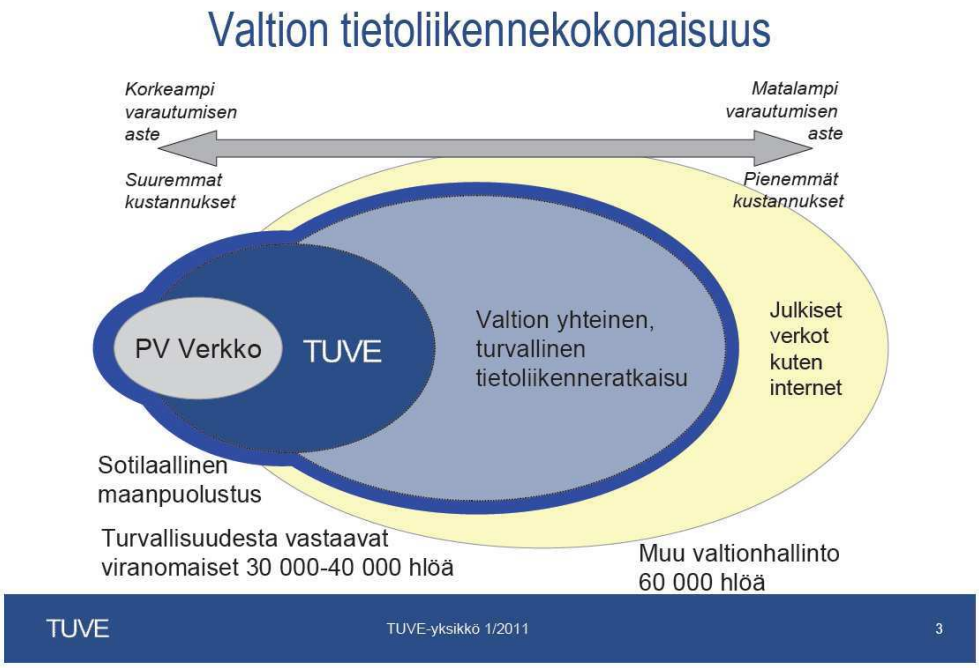
(Viestintämarkkinalaki 393/2003 9:90-99 §).

2.4 TUVE vaikutukset

Hallinnon turvallisuusverkkohanke (TUVE) hankkeessa todetaan, että Puolustusvoimat tulee toimimaan osana eri valtionhallinnon palveluja käyttävien viranomaisten tietoliikenneoperaattorina. Tämän johdosta on PSJJK:n pystyttävä omalla alueellaan reagoimaan entistä nopeammin ja tehokkaammin tuottamiensa palveluiden ja järjestelmien ylläpidon osalta. Tässä työssä tarkastellaan TUVE- kehitysvaiheen tasoa 1: ”Yhteinen verkko” (kuva 1), joka käsittää siirtoyhteydet. (Valtionvarainministeriön www-sivut 2011, hakupäivä 30.11.2011).

Kuva 1. VMTUVE hankkeen kehitysvaiheet (VMTUVE Valtionvarainministeriön www-sivut 2011, hakupäivä 30.11.2011)

Viime vuosina PSJJK:n organisaation henkilöstö on ollut voimakkaassa muutosvaiheessa. Tehtäviä on siirretty eri organisaation sisällä eri paikkakunnille, tai henkilöstö on omatoimisesti siirtynyt eri tehtäviin PSJJK:n organisaatiosta. Lisäksi henkilöstöä on siirtynyt myös muille työnantajille. Nämä muutokset eivät vielä ole suoranaisesti vaikuttaneet PSJJK:n kykyyn ylläpitää järjestelmiä, mutta vaikutusta tulee kuitenkin arvioida yleisellä tasolla.



Kuva 2. Valtion tietoliikennekokonaisuus (Valtionvarainministeriön www-sivut 2011, hakupäivä 30.11.2011)

Puolustusvoimien verkko on osana koko valtion hallinnon viranomaisten tiedonsiirtoverkkoa (kuva 2), joten sen verkon toimivuudelle asetetaan suuret vaatimukset. Näin ollen myös poikkeusoloihin perustuvan varautumisasteen tulee olla huomattavasti korkeampi, kuin tavallisten julkisten verkkojen varautuminen. Kustannuksia verratessa varautumistason mukaan matalamman tason varautumisessa palvelukriittisyys ei ole niin suuri, kuin valtionhallinnon viranomaispalveluiden toimivuus. Tämän vuoksi korkeammasta varautumisasteesta johtuen verkon ylläpitokustannukset tulevat kasvamaan normaalia verkon ylläpitoa korkeammaksi.

Opinnäytetyön käsittelyosa rakentuu aiheen, tavoitteen ja toteutustavan mukaisesti. Selostuksessa edetään johdonmukaisesti. Sisältö jäsennellään pää- ja alaotsikoinnilla sekä muilla tehokeinoilla. Sisällön rakentamisessa käytetyt lähteet osoitetaan lukijalle riittävän selvästi jäljempänä annettavien ohjeiden mukaisesti.

3 RISKIT JA STRATEGINEN KOKONAISTURVALLISUUS

Organisaation kokonaisturvallisuudessa käsitellään usein käsitteitä uhka ja riski. ”Uhka” terminä liitetään usein sotilaalliseen toimintaan ja käsite ”riski” liitetään yritysmaailman liiketoiminnan ajatteluun. Organisaation kokonaisturvallisuus on kuitenkin uhkien ja riskien hallintaa. Yleisesti voidaan todeta, että uhka on vaaran, sen vaikuttavuuden ja riskin tulo. (Mäkinen 2007, 107).

Riski on vahingon sattumisen mahdollisuus. Riskit syntyvät yleensä ihmisen aiheuttamien toimenpiteiden johdosta, ja näin ollen niihin voidaan vaikuttaa ja varautumisen toimenpitein niiltä voidaan myös suojautua. Riskien tunnistaminen on riskinhallinnan perusasia. Tunnistamattomia riskejä ei voi hallita. Tarkoituksena on ennakoida riskit ja huolehtia toimenpitein siitä, etteivät ne pääse yllättämään. Yleensä yritystoiminta edellyttää, että riskejä otetaan järkevästi, esimerkiksi ajan, vaivan ja rahan säästämiseksi. (PK-RH www-sivut 2012. Hakupäivä 13.10.2012).

Kokonaisturvallisuuteen liittyviä yhteiskunnan toiminnoille tärkeimpiä infrastruktuureja kutsutaan kriittisiksi infrastruktuureiksi. Yksi kriittisistä infrastruktuureista puolustusvoimissa, on tietoliikenneyhteyksien toimivuus. Riskien luokittelun avulla pyritään parantamaan PSJJK:n riskitietoisuutta, ja näin ollen pyritään paremmin ennakoimaan tietoliikennejärjestelmiin kohdistuvat mahdolliset uhat järjestelmien toiminnan kannalta.

3.1 Riskikategoriat

Riskien luokittelu on riskinhallinnan perusasia, jonka avulla riskien vaikutusta voidaan vertailla keskenään paremmin. Riskien luokittelun avulla pyritään varmistamaan se, että yrityksessä on tarkasteltu mahdollisimman kattavasti kaikkia niitä tekijöitä, jotka vaikuttavat yrityksen toimintaan.

Riskien jaottelussa on useita eri tapoja. Yksi yleisimmistä tavoista on jakaa riskit neljään riskilajiin: strategiset riskit, taloudelliset riskit, operatiiviset riskit ja vahinkoriskit. (Taulukko 1). Tässä tapauksessa riskit jaetaan tyypin mukaan ja niiden tekijöiden, joiden vaikutuksesta riski toteutuu. (Ilmonen, Kallio, Koskinen &Rajamäki 2010, 70).

Taulukko 1. Riskikategoriat mukailtu (Ilmonen ym. 2010, 71)

Strategiset riskit	**Taloudelliset riskit**	**Operatiiviset riskit**	**Vahinkoriskit**
Teknologiariskit	Likvideettiriskit	Informaatioteknologiaan liittyvät riskit	Työterveys- ja työturvallisuusriskit
Liiketoiminnan kehitykseen liittyvät riskit	Sopimusriskit	Tietoturvariskit	Henkilöstöriskit
Liiketoimintaympäristöön liittyvät riskit	Valuuttariskit	Kriisitilanteisiin liittyvät riskit	Ympäristöriskit
Markkinariskit	Korkoriskit	Organisaatioon ja johtamiseen liittyvät riskit	Luonnonkatastrofeihin liittyvät riskit
Regulaattoririskit	Maariskit	Rikosriskit	Toimitilaturvallisuusriskit

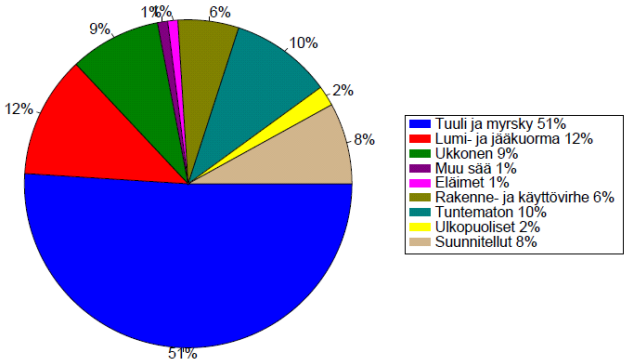
Strategisilla riskeillä ymmärretään muutoksia, jotka vaikuttavat yrityksen pitkän aikavälin strategisiin tavoitteisiin. Usein niistä käytetään myös nimitystä liiketoimintariski. Strategiset riskit osuvat liiketoimintaympäristön epävarmuustekijöihin ja saattavat olla joko sisäsyntyisiä, tai kohdistua yritykseen sen ulkopuolelta.

Yritysjärjestelyihin ja yrityskauppoihin liittyvät riskit voivat olla merkittäviä yritykselle tarkasteltaessa sen kykyä tuottaa palveluja. Yritys voi fuusioitua toiseen organisaatioon, jolloin yrityksen liiketoimintamahdollisuus voi muuttua merkittävästi. (Ilmonen ym. 2010, 71-72).

Operatiiviset riskit liittyvät yrityksen jokapäiväiseen toimintaan, koostuen välittömistä tai välillisistä tapahtumista. Nämä voivat olla seurausta yrityksen epäonnistuneista sisäisistä prosesseista tai ulkoisista tapahtumista. Tietoturvallisuuteen liittyviä riskejä ovat tiedon eheyteen, saatavuuteen ja luottamuksellisuuteen kohdistuvat toimenpiteet. Merkittävimmät operatiiviset riskit ovat liiketoiminnan keskeytykseen johtavat riskit, joita voivat aiheuttaa työntekijöiden lakkoilu, tulipalot tai konkurssit. Tällaiset tapahtumat voivat olla joko ulkoisia tai sisäisiä. (Ilmonen ym. 2010, 72-73).

Taloudellisia riskejä ovat yrityksen rahaprosesseihin liittyvät riskit, kuten likviditeettiriskit, korkoriskit ja pääomarakenteeseen liittyvät riskit. Lisäksi myös erilaiset sopimusriskit, sekä osa maariskeistä luetaan kuuluvaksi taloudellisiin riskeihin. (Ilmonen ym. 2010, 74-75).

Tietoliikenneyhteyksiä tuottavassa yrityksessä vahinkoriskit toteutuvat useimmin, ja näin ollen niistä aiheutuviin palvelupoikkeamiin tulee varautua riittävän huolellisesti. Tyypillisiä vahinkoriskejä ovat henkilöstöön liittyvät sairastumiset, poissaolot, avainhenkilöiden poistumiset, osaamiseen liittyvät asiakokonaisuudet ja niin edelleen. Luonnonkatastrofit ovat merkittävimpiä tiedonsiirtojärjestelmiin vaikuttavia riskejä, esimerkiksi sähkökatkot (kuva 3).



Kuva 3. Sähkökatkojen aiheuttajat vuonna 2010 (Energiateollisuuden www-sivut 2011. Hakupäivä 4.5.2012)

Kuten riskejä jaotellessa huomataan, ovat eri ryhmiin kuuluvat riskit osin hyvin samankaltaisia toisilleen, ja näin ollen samaan asiaan liittyy sekä strateginen, että operatiivinen taso. (Ilmonen ym. 2010, 75).

3.2 Riskin hallinta

Riskienhallinnassa on neljä selkeää päävaihetta, jotka PK-RH on määritellyt seuraavasti:

1. Riskien tunnistaminen ja arviointi

Riskin tunnistaminen on haastava osa yrityksen kokonaistoimintaa, koska sen tulee kattaa koko yrityksen toiminta. Näin ollen se vaatii paljon yhteistyötä eri henkilöiden kanssa. Tarkoituksena on löytää ne riskit, joita ei arkisessa työssä ole huomattu. Yleensä tässä vaiheessa käsitelläänkin kerrallaan vain osaa yrityksen toiminnasta, ja myöhemmin jatketaan jonkin toisen osa-alueen tarkastelua.

2. Riskien torjunnan suunnittelu ja toimenpiteet

Tässä mietitään, miten vahingot voidaan välttää, pienentää, siirtää tai pitää. Käytännön toimenpitein tehdään suoritteita, joilla riskejä voidaan vähentää. Riskien torjunta on syytä aloittaa suurimmaksi arvioidusta riskistä ja ulottaa mahdollisimman laajalle.

3. Varautuminen vahinkoihin

Vahinkojen sattumiseen on syytä varautua ja pyrkiä varmistamaan toiminnan jatkuminen myös ongelmatilanteissa. Vahingon sattuessa on liian myöhäistä miettiä ja suunnitella, mitä tulisi tehdä. Yrityksen kehittämät varajärjestelmät ovat avainasemassa näissä tapauksissa.

4. Tilanteen seuranta ja oppiminen

Yrityksissä seurataan usein esimerkiksi poissaolojen määrää ja syitä, tuotantokatkojen pituuksia ja mahdollisten tuotantovirheiden laatua. ”Läheltä piti”-tilanteet tulisi aina tutkia ja niistä pitäisi ottaa oppia myöhempiä toimintoja varten.

3.3 Riskiarvio

Riskiarviota tehtäessä, riski määritellään yleisesti riskin todennäköisyyden ja riskin vakavuuden tulona. Todennäköisyyttä arvioitaessa voidaan tyypillisten ja jo havaittujen tapahtumien perusteella tehdä tarkkojakin arvioita, mutta mahdollisten uusien esimerkiksi liiketaloudellisiin liittyvät todennäköisyydet ovat vaikeampia arvioida.

Tämän yleisen riskikaavan määrittelyn ongelma on se, että se ei aseta riskejä tärkeysjärjestykseen sen mukaan miten niihin tulisi varautua (taulukko 2). Mikäli riskin todennäköisyys on suuri, mutta vakavuus on merkityksetön, aiheuttaa se yleensä pientä taloudellista menetystä ja pientä häiriötä tietoliikennepalveluissa. Toisaalta, jos riskin todennäköisyys on pieni, mutta vakavuus on merkittävä, aiheutuu tällöin liiketoiminnalle ja tietoliikennepalveluille isot häiriöt, jos tähän ei ole varauduttu.

Taulukko 2. Yleinen riskikaava, mukailtu (Mäkinen 2007, 111).

Riskiarvio	Uhka toiminnan jatkuvuudelle
< 10	Vähäinen riski
10-20	Kohtalainen riski
> 20	Merkittävä riski
kaava	Riski = todennäköisyys x vakavuus, (arvot, välillä 1-5)

Mikäli yleistä riskikaavaa halutaan mukauttaa omaa toimintaympäristöä ajatellen, voidaan taulukko esittää seuraavassa muodossa.(Taulukko 3)

Taulukko 3. Oma riskiarvio

Riskiarvio	Uhka toiminnan jatkuvuudelle
<5	Merkityksetön riski
5-10	Vähäinen riski
11-15	Kohtalainen riski
16-20	Merkittävä riski
> 20	Sietämätön riski
kaava	Riski = todennäköisyys x vakavuus, (arvot, välillä 1-5)

Riskin todennäköisyyden määrittely yleisessä riskikaavassa on esitetty taulukossa 4.

Taulukko 4. Riskin todennäköisyys, mukailtu (Mäkinen 2007, 108).

Luokka	Selite
1	Erittäin harvinainen riski, korkeintaan kerran 50 vuodessa
2	Harvinainen riski, kerran 25 vuodessa
3	Melko harvinainen riski, kerran 10 vuodessa
4	Melko todennäköinen riski, kerran vuodessa
5	Erittäin todennäköinen riski, useita kertoja vuodessa

Riskin vakavuuden arviointi riippuu yrityksen riskinkantokyvystä, joka pienillä yrityksillä saattaa olla heikko, jos tuotteita on vähän ja ollaan sen toimivuuden varassa. Riskinkantokyky vaihtelee yrityksessä sen taloudellisen tilanteen ja tuotevalikoiman muuttuessa. Tämän vuoksi riskinkantokyky tulisikin määritellä yrityksessä säännöllisesti. Riskin vakavuus voidaan esittää yleisellä tasolla seuraavasti. (Taulukko 5)

Taulukko 5. Riskin vakavuus, mukailtu (Mäkinen 2007, 109).

Luokka	Selite
1	Vähäinen vaikutus toimintakykyyn, hetkelliset toimintahäiriöt, ei toiminnan keskeytymistä.
2	Pieni vaikutus toimintakykyyn, toiminta häiriintyy osittain, lyhyt toiminnan keskeytyminen.
3	Kohtalainen vaikutus toimintakykyyn, toiminta häiriintyy laajamittaisesti, toiminta keskeytyy määräajaksi.
4	Suuri vaikutus toimintakykyyn, toiminta lakkaa toistaiseksi.
5	Katastrofaalinen vaikutus toimintakykyyn, toiminta lakkaa kokonaan, huomattavan suuri ja pitkälle tulevaisuuteen ulottuvia vaikutuksia.

Tässä työssä keskitytään siihen, kuinka PSJJK:ssa pyritään kehittämään kykyä tunnistamaan ne riskit, jotka voivat vaikuttaa tiedonsiirtojärjestelmien toimintaan eri tilanteissa. Työssä syntyneessä riskianalyysissä (Liite 1) ei voitu suoraan käyttää perinteisiä riskin vaikuttavuuden arvoja, vaan joillekin laadittiin omat erilliset arvot. Muutetuista arvoista on selitykset annettu aina kohdekohtaisesti. Liitteen julkisuuden vuoksi asioita käsitellään sillä tasolla, että niitä voidaan julkaista tässä työssä.

4 KUNNOSSAPITO

4.1 Kunnossapidon määrittely

Kunnossapidolla käsitetään erilaisten asioiden, kuten laitteiden, koneiden, järjestelmien, rakennusten tai prosessien toimintakuntoisuuden ylläpitämistä. Tämän johdosta kunnossapidon suhde huoltoon on paljon merkityksellisempi ja laajempi kokonaisuus, ja näin ollen sen merkitys kasvaa entistä enemmän yrityksen kilpailukyvyn takaamiseksi (Järviö 2004, 12). Standardeissa kunnossapito määritellään seuraavasti:

> *”Kunnossapito koostuu kaikista kohteen eliniän aikaisista teknisistä, hallinnollista ja liikkeenjohdollisista toimenpiteistä, joiden tarkoituksena on ylläpitää tai palauttaa kohteen toimintakyky sellaiseksi, että kohde pystyy suorittamaan vaaditun toiminnon”*. (SFS-EN 13306, 54)

> *”Kunnossapito on kaikkien niiden teknisten, hallinnollisten ja johtamiseen liittyvien toimenpiteiden kokonaisuus, joiden tarkoituksena on säilyttää kohde tilassa tai palauttaa se tilaan, jossa se pystyy suorittamaan vaaditun toiminnon sen koko elinjakson aikana”*.(PSK 6210, 36)

4.2 Kunnossapidon organisoiminen

Kunnossapidon organisoiminen ja toimintamallien laatiminen riippuu yrityksen politiikasta, koosta, tuotantostrategiasta sekä ulkopuolisten palvelujen saatavuudesta. Kunnossapito voidaan jakaa seuraaviin periaatemalleihin:

- keskitetty kunnossapito
- hajautettu kunnossapito
- kunnossapito omana tulosyksikkönä
- kunnossapidon osto alihankintana
- käynnissäpito, pieni oma kunnossapito-osasto
- edellä mainittujen kohtien erilaisia yhdistelmiä.

(Aalto 1994, 33)

Keskitetyssä järjestelmässä kunnossapito toimii omana erillisenä keskitettynä organisaationaan. Keskitetyssä kunnossapidossa voidaan saavuttaa seuraavia etuja, jotka tukevat yrityksen toimintaa.

Työvoimaresurssi on yhtenäistä ja helposti siirrettävää.

- Henkilöstö osaaminen voidaan keskittää ja koulutusta järjestää heloposti omalle henkilöstölle.
- Hankittua erikoisosaamista voidaan käyttää kokoko yrityksen hyväksi niin kunnossapidon kuin suunnittelun sekä asentamisen töissä.
- Tiedonhallinta pysyy yrityksen sisällä ja johtaminen on selkeää koska henkilöstö on omaa. Tiedon seuraaminen on tehokasta, voidaan pitää ajantasaisena.

(Aalto 1994, 33)

Keskitetyssä organisaatiossa saattaa ilmetä myös varjopuolia joita on seuraavissa osa-alueissa:

- Keskitetty organisaatio saattaa olla jäykkä, koska resursseja jaetaan myös muihin töihin, ja näin ollen resurssi ei ole tehokkaasti käytettävissä kunnossapidon puolella.
- Isoissa yrityksissä saattaa organisaatio olla tehoton ja hidas.
- Isoissa organisaatioissa yksittäisten osastojen ongelmat saattavat jäädä huomaamatta ja niistä aiheutuvat vaikeudet voivat tulla yllätyksenä yrityksen johdolle.

(Aalto 1994, 33)

Hajautetussa järjestelmässä kunnossapito toimii yleensä yrityksessä suoraan omana alayksikkönä tuotannon alaisuudessa. Tämän vuoksi voi tuottaa nopeasti ja joustavasti kunnossapitopalveluja. Yksikön henkilöstön osaaminen on erikoisosaamista ja pystyy vaativiin ongelmien ratkaisuihin. Toisaalta henkilöstön joustava käyttö on vaikeammin toteuttavissa kuin keskitetyssä järjestelmässä.

Omana yksikkönä toimiessaan kunnossapito pyrkii kustannustehokkaaseen toimintaan, sekä kustannusten karsimiseen. Koska yksiköllä on oma eriytetty toiminta ja kustannuslaskenta nähdään kustannusvaikutuksena pelkästään tulosyksikön kannalta, aiheuttaa se hiukan lisää byrokratiaa. Palvelu- ja asiakassuhteen luominen tuo palvelualttiutta toimintaan, sekä kilpailuttamismahdollisuus pitää yllä halua tehokkaaseen toimintaan.

Osaavien henkilöiden aiheuttama resurssien haavoittuvuus tulee huomioida riskinä hyvin yrityksen toimintatavoissa ja strategiassa. Tämän vuoksi alihankinnalla pyritään kapasiteettihuippujen tasaamiseen tai mahdollisten erityisosaamista vaativien töiden teettämiseen. Alihankintana saatetaan ostaa lisäksi standardilaitteiden koko kunnossapito esimerkiksi tietojärjestelmä, tulostinpalvelu tai matkapuhelimien ylläpito.

Kunnossapidon yhtiöittäminen ja palveluiden ostaminen uudelta perustettavalta yhtiöltä tai koko kunnossapito osa-alueen ostaminen palveluna on myös vaihtoehto. Ostopalvelun etuja on se, että maksetaan vain siitä, mitä käytetään kunnossapitoresursseihin. Kunnossapito voidaan kilpailuttaa ja näin ollen voidaan saavuttaa tehokkaampaa kustannuskontrollia. Ostopalveluiden haittapuoliksi voidaan katsoa se, että yrityksen oman henkilöstön ammattitaito ja osaaminen katoavat ulkopuoliselta ostetun kunnossapidon osalta. Näin ollen oma erikoisosaaminen heikkenee. Lisäksi oma yritys ei voi vaikuttaa täysin niihin resursseihin, jotka tekevät ulkoistettua kunnossapitoa. Tästä saattaa aiheutua viivettä ja yhteistyöongelmia.

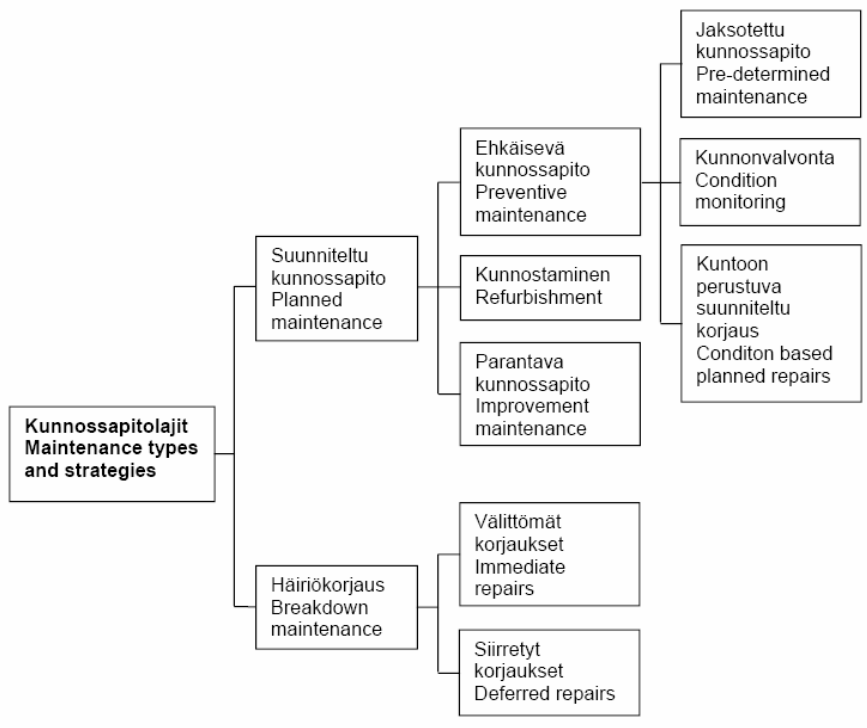
Käynnissäpito, oman toimen ohessa suoritettava kunnossapito, on pienissä yrityksissä hyvin yleinen toimintatapa. Kun yrityksen kunnossapito ei kata täysipäiväisesti erillisen kunnossapitohenkilöstön kokoaikatyötä, on tällainen järjestely edukasta. Tämä toimintatapa soveltuu isoissakin yrityksissä, missä toimitaan itsenäisessä yksikössä yksinkertaisilla laitteilla. (Aalto1994, 13-24).

4.3 Kunnossapidon osa-alueet

Kunnossapito jaetaan yleisesti ehkäisevään kunnossapitoon ja korjaavaan kunnossapitoon. Toiminnot, jotka suoritetaan ennen kuin laitteen toiminta pysähtyy vikaantumisen vuoksi, ovat ehkäisevää kunnossapitoa. Vian vuoksi laitteelle tehtävä korjaus on korjaavaa kunnossapitoa. (SFS-EN 13360, 24).

Kunnossapito voidaan jakaa myös suunniteltuun kunnossapitoon ja häiriökorjauksiin. Tämä jako on tehty prosessiteollisuuden näkökannalta, PSK 7501 standardi. PSK ja SFS-EN standardi ovat samanhenkisiä, jako on vain erilainen. (Järviö 2004, 38)

Kunnossapidon toteuttamisessa suunnitellun ja häiriökorjauksen välisen kunnossapidon osalta pääpaino tulisi olla ehkäisevässä kunnossapidossa. Ehkäisevän kunnossapidon osalta tulee huomioida, ettei siihen kuitenkaan suunnata liikaa resursseja, koska kuitenkin vikatapauksia tulee ja niihinkin tulee olla resursseja. Kuvassa 4 on esitetty mihin eri kokonaisuuksiin kunnossapitolajit jakautuu.

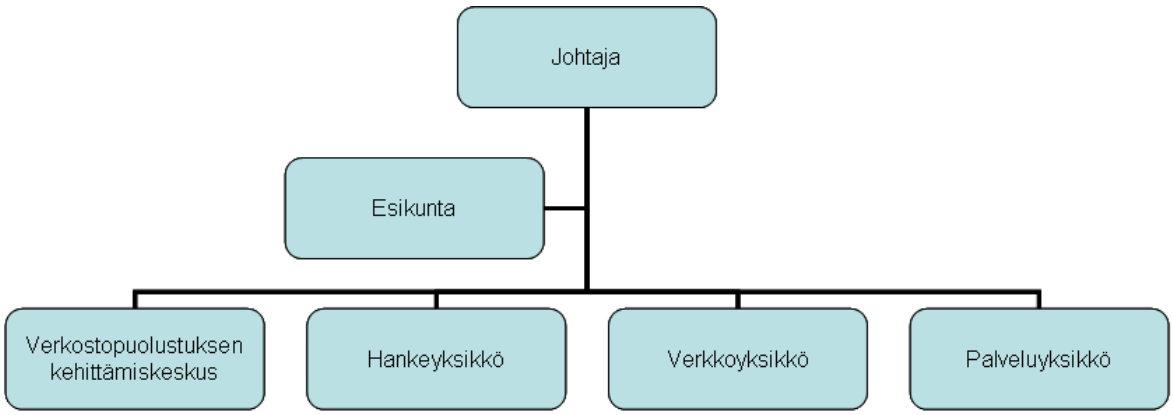


Kuva 4. Kunnossapitolajit, mukailtu (Järviö 2004, 39)

5 ORGANISAATIO JA HENKILÖSTÖ

5.1 Organisaatiorakenne

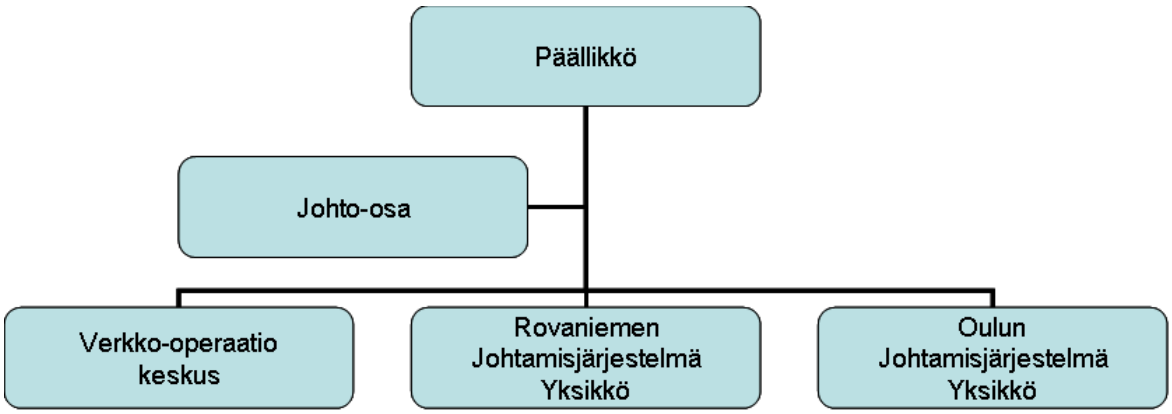
PVJJK on Pääesikunnan alainen laitos, joka on aloittanut toimintansa vuoden 2007 alussa. Johtamisjärjestelmäkeskus toimii kahdellakymmenelläkahdella paikkakunnalla. Tärkeimmät osat, kuten johto, Esikunta ja Verkkoyksikön johto, ovat sijoittuneet Jyväskylään. Hankeyksikkö sijaitsee Espoossa ja Verkostopuolustuksen kehittämiskeskus Riihimäellä. Palveluyksiön johto sijaitsee Tampereella. (Kuva 5). (Puolustusvoimien www-sivut 2012. Hakupäivä 3.1.2012).



Kuva 5. PVJJK organisaatiorakenne (Puolustusvoimien www-sivut 2012. Hakupäivä 3.1.2012)

Johtamisjärjestelmäkeskuksen tärkein tehtävä on mahdollistaa puolustusvoimien operatiivinen johtaminen valmiuden kohottamisen kaikissa vaiheissa. Lisäksi Johtamisjärjestelmäkeskuksen päätehtäviin kuuluu Puolustusvoimien ITVJ (integroidun tiedustelu-, valvonta- ja johtamisympäristön) kehittäminen ja ylläpitäminen sekä hallinnollisten tietohallintopalveluiden tuottaminen koko puolustushallinnolle, sekä soveltuvin osin myös muulle valtionhallinnolle. (Puolustusvoimien www-sivut 2012. Hakupäivä 3.1.2012).

PSJJK kuuluu Verkkoyksikköön, ja on näin ollen osa PVJJK:n organisaatiota. Keskuksen toiminta-alue kattaa koko Pohjois-Suomen sisältäen Oulun- ja Lapinlääninn, lisäksi keskus tuottaa palveluja kansainvälisille joukoille.(Kuva 6), (Puolustusvoimien www-sivut 2012. Hakupäivä 3.1.2012).



Kuva 6. PSJJK organisaatiorakenne (Puolustusvoimien www-sivut 2012. Hakupäivä 3.1.2012)

5.2 Henkilöstön käyttö

PSJJK toimii pääosin suoraan linjaorganisaatiossa, jossa työnjohto ja hallinto tulevat ylemmältä taholta. Toisaalta osa töistä tehdään matriisiorganisaatiomallilla, jolloin henkilöstöä voidaan käyttää ristiin eri projekteissa. Monesti tämä matriisiorganisaatiomalli onkin välttämätön, koska keskus suorittaa alueellaan rakentamisen ja ylläpidon samalla henkilöstöllä.

Organisaatiosta ei ole eriytetty eri henkilöitä kunnossapidon puolelle, vaan samat henkilöresurssit suorittava niin rakentamisen kuin kunnossapitoon kuuluvat tehtäväkokonaisuudet. Tehtäviä ohjaavat eri lait, asetukset, määräykset ja laitevalmistajien ohjeet. Lisäksi organisaation sisällä on laadittu erilaisia toimintatapoja kunnossapidon ylläpitämiseen saatujen kokemuksien pohjalta.

PSJJK:n toiminnan kannalta haasteellisuutta tietoliikenneverkkojen ylläpidon osalta luo laaja toimintaympäristö, pitkät etäisyydet ja vaihtelevat sääolosuhteet sekä pitkä talvikausi. Nämä erikoisvaateet vaativat henkilöstöresurssien sekä materiaalin käytöltä tarkkaa suunnittelua ja hallintaa.

6 OSAAMINEN

Henkilöstön osaamisella on organisaation näkökannalta merkittävä painoarvo siirryttäessä toimimaan normaaliolosta poikkeusolotilanteeseen. Tällöin yksilö joutuu toimimaan mahdollisesti erilaisessa työympäristössä tai suuremman vastuun alla kuin normaalityötehtävissä. Mitä vaativampi osaamisalue on, sitä merkittävämmässä osassa on henkilön osaaminen ja kyky toimia ryhmässä. Tämän vuoksi onkin jo normaaliolonaikana kiinnitettävä riittävällä tasolla organisaatiossa osaamisen ylläpitämiseen.

6.1 Yksilöosaaminen

Yksilön osaaminen koostuu henkilön tiedoista, taidoista, kokemuksista, kontakteista, asenteesta ja henkilökohtaisista ominaisuuksista, joiden avulla henkilö selviää tehtävästään ja saavuttaa tavoitteensa. Yksilön taidot ja tiedot on hankittu ajan mittaan koulutuksella, opiskelulla ja tekemisen avulla. Henkilön persoona ja motivaatio sekä asenteet ovat koetuksella, kun organisaatiossa pyritään jatkuvaan muutokseen ja sopeutumiseen uusiin tilanteisiin. Henkilön sosiaaliset taidot määrittää usein myös sen, kuinka hyvin tulee toimeen oman työyksikkönsä ja muiden henkilöiden kanssa. (Otala 2008, 50-51).

6.2 Organisaation osaaminen

Yksilöiden osaaminen muuttuu organisaation osaamiseksi, kun henkilöt jakavat, yhdistelevät sekä kehittävät yhdessä osaamistaan. Yrityksessä henkilöt usein ovat hajallaan eripuolilla organisaatiota ja näin ollen osaaminen koostuu hajautuneesta asiantuntijuudesta, joka tulee saattaa johtamisella, toimintatavoilla ja organisaatiorakenteilla yhteen.(Otala 2008, 53).

Organisaatiossa on tärkeintä pitää työntekijöiden innostus ja heidän energia huipussaan, jolloin päästään erinomaisiin tuloksiin. Innostuksen perusmalleja on ”työn imu”-teoria, jossa työntekijä pystyy panostamaan senhetkiseen tehtäväänsä koko energiansa. (Otala & Pöysti 2012, 229).

6.3 Ammatillinen osaaminen

Ammatillista osaamista voidaan selvittää tekemällä henkilöstölle osaamiskartoitus (Liite2). Kartoituksen tarkoituksena on saada selville henkilöstön nykyinen ammattitaito ja verrata sitä siihen, mitä nykyiset tehtävänkuvaukset vaativat. Kartoituksen perusteella voidaan laatia tarkemmat jatkosuunnitelma henkilöstön kehittämisen tueksi.

6.4 Tiimiosaaminen

Tiimiosaamisella tarkoitetaan henkilöstön kykyä toimia lähimmässä työtiimissään sekä laajemmassa kokonaisuudessa koko PSJJK:n organisaatiossa. Vuorovaikutustaitojen kartoittaminen on laajemmassa mittasuhteessa haastava tehtävä.

Tiimityöskentelyä voidaan arvioida PSJJK:ssa tehtävästä työilmapiirikyselystä, josta saadaan selville, millä tavoin työyksiköissä aistitaan henkilöiden keskinäinen toimivuus. Työilmapiirikyselyssä saadaan selville myös henkilöstön näkemys organisaation toimivuudesta ja tavoitteiden asettelusta. Mikäli organisaatiossa ei tehdä työilmapiirikyselyjä, voidaan organisaation toimintakulttuurista saada toimintatapojen tärkeys esiin tekemällä oppivan organisaation testi esimerkiksi Otalan mallilla. (Otala 2008, 339).

6.5 Oppiva organisaatio

Oppivassa organisaatiossa pelkästään osaamisen kehittäminen ei riitä, vaan pitää luoda olosuhteet, jossa yksilön oppimien muuttuu organisaation osaamiseksi. Näin ollen yrityskulttuurista tulisi luoda oppimiskulttuuri. (Otala 2008, 278)

Oppimismyönteisen yrityskulttuurin tyypilliset piirteet ovat:

- avoin ilmapiiri ja luottamus
- innostava ja energiasoiva
- uteliaisuutta herättävä ja kannustaa hakeman uusia ratkaisuja
- positiivinen tunnelma ja rakentava kritiikki ovat sallittua
- tehdyt virheet ovat oppimismahdollisuuksia ja niitä käsitellään avoimesti
- hiljaisen tiedon siirtymisen tukevaa
- houkuttaa ylittämään mukavuusrajan
- arvostaa kaikkien näkökantoja ja kannustaa tekemään uusia esityksiä ja ideoita

- jokainen tuntee kunnioitusta ja tuntee tulleen kuulluksi
- innostaa kysymään ja kyseenalaistamaan
- korostaa yhteisöllisyyttä.

6.6 Hiljaisen tiedon siirtäminen

Luottamuksellinen ilmapiiri organisaatiossa on tärkeä osa tiedon jakamisen edistämisessä. Vastuun jakaminen usealle henkilölle yrityksessä vähentää mahdollisesti sisäistä kilpailua, ja näin ollen tehostaa hiljaisen tiedon jakamista ja hyödyntämistä organisaatiossa. Jatkuvat muutokset ja tuotannossa tapahtuvat supistukset lisäävät epävarmuuden tunnetta ja ovat omiaan estämään oman tiedon jakamisen mahdollisille kilpailijoille työyhteisössä. (Otala 2008, 280).

Hiljaisen tiedon jakamisessa on tärkeää jakajan motivaation ylläpitäminen. Hiljaisen tiedon siirtyminen toteutuu ainoastaan silloin, kun henkilöt pystyvät jakamaan omia tietojaan ja kokemuksiaan positiivisessa ja hyväksyvässä ympäristössä.

Luottamuksen lisäämiseksi ryhmässä olisi hyvä, jos henkilöt voisivat toimia samassa ryhmässä pitkään. Näin he oppisivat tuntemaan toisensa ja luottamus ryhmän sisällä kasvaisi, mikä taas lisäisi tiedon jakamista, mikäli työnjohto mahdollistaisi sisäistä työnkiertoa ryhmän sisällä. Työnkierto ei saisi kuitenkaan olla kilpailevaksi ymmärrettävää, vaan yhteisen päämärän tavoittelemista. Näin ollen myöhemmin mahdollisissa organisaation ryhmämuutoksissa saadaan mahdollisimman paljon tietoa jaettua.

Organisaation palkitsemiskulttuuria pitäisi kehittää: palkittaisiin mieluummin ryhmien aikaansaamisia kuin yksilöitä. Tällöin kannustettaisiin jokaista tuomaan omaa osaamistaan paremmin esille ryhmässä ja näin tieto jakaantuisi ryhmän sisällä tehokkaammin.

7 KRIITTISTEN KOHTEIDEN MÄÄRITTELY

Organisaation ylläpitämien tietoliikenneverkkojen ja palveluiden tulee olla käytettävissä niin normaaliajan olosuhteissa, kuin myös poikkeusoloissa. Tähän varautuminen asettaa erityisiä vaatimuksia tuottaa poikkeusolojen palveluja. Tässä työssä tutkittiin eräitä puolustusvoimien kannalta katsottuja mahdollisia tärkeitä toimintoja, joiden ylläpitämiseen on kiinnitettävä huomiota.

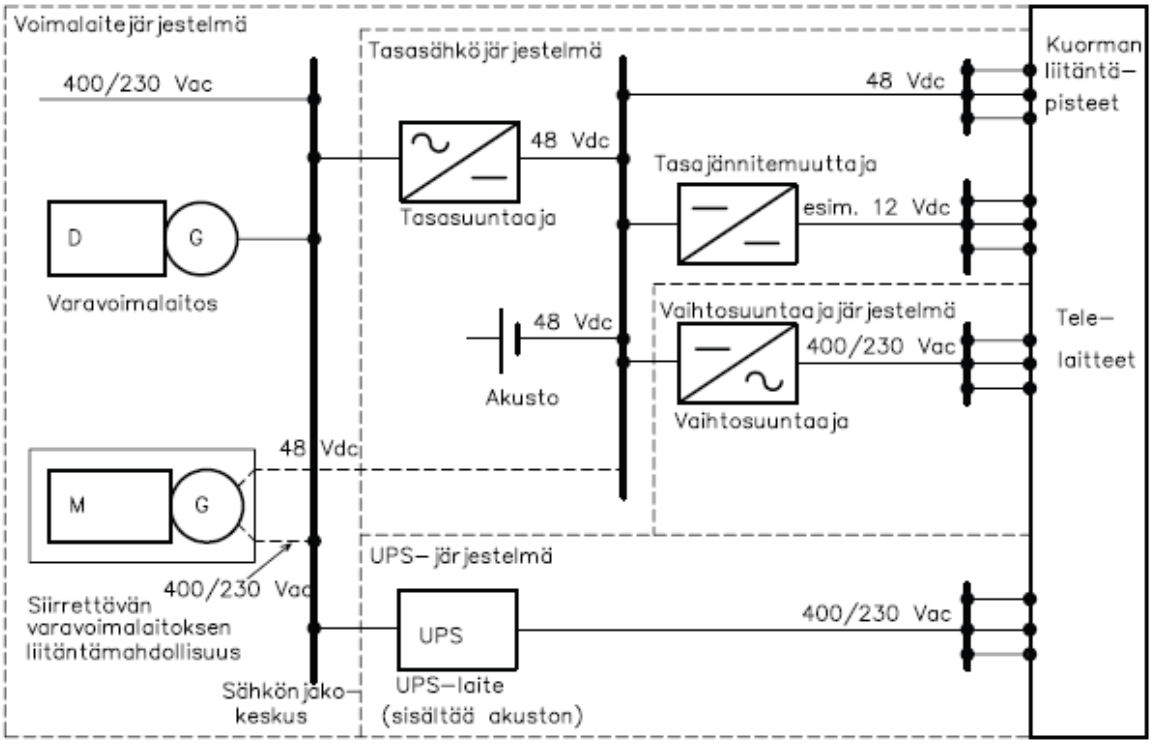
Jokainen organisaatio pystyy omalta osaltaan määrittelemään omia mahdollisia kriittisiä kohteita, joita haluaa oman toimintansa kannalta seurata. Näiden valittujen kohteiden osalta voidaan miettiä suoraan organisaation riskinkantokykyä.

7.1 Kohteen sähköistys

Valtakunnan sähköverkko ja alueellisten sähköyhtiöiden jakeluverkko ei kaikissa olosuhteissa pysty takaamaan keskeytymätöntä sähkönsyöttöä, joten tietoliikenneverkon toimivuuden kannalta tärkeimmät viestiasemat on rakennettava siten, että niiden tehonsyöttö on varmistettu ja ne toimivat myös poikkeusoloissa. Organisaation toiminnassa tulee määritellä ne viestiasemat ja tietoliikennelaitteet, joiden tulee pystyä toimimaan myös poikkeustilanteissa, ja näin ollen ne tukevat organisaation suorituskykyä ja velvoitteita. Varautumisessa tulee organisaation määrittä, missä laajuudessa ja kuinka kauan sähkönsyöttö tulee kohteessa varmentaa. Sähköhäiriöt pääsääntöisesti johtuvat joko laitevioista tai luonnon aiheuttamista vahingoista, mutta myös mahdollisiin sotatilan aiheuttamiin vikoihin tulee varautua.

Sähkönjakelun häiriöt voidaan jakaa periaatteessa neljään kategoriaan:
– lyhyet katkokset käsittäen pika- ja aikajälleenkytkennät sekä käyttötoimenpiteet
– pitkät katkokset sähkön jakelussa esim. vikakorjausten ajaksi
– jännitteen laatupoikkeamat, kuten jännite- ja taajuusvaihtelut sekä transienttiylijännitteet
– sähkönjakelun keskeytyminen useiksi tunneiksi tai vuorokausiksi laajoissa vikatilanteissa tai tehonvajauksessa. (Sähköinfo OY:n www-sivut 2012. Hakupäivä 3.11.2012).

Tärkeimpien viestiasemien sähkönsyöttö pitäisi saada rakennettua siten, että jakeluverkon syöttö saadaan tuotua viestiasemalle kahden eri muuntajapiirin ja erillisten syöttölinjojen kautta. Lisäksi kohde tulee varmentaa lyhyitä sähkönsyötön katkoksia varten joko akkuvarmennus, tai UPS laitteistolla viestiasemalla olevista laitejärjestelmistä riippuen. Pitkäkestoisia katkoksia varten viestiasema on varustettava kiinteällä varavoimakoneistolla ja siirrettävän varavoiman syöttömahdollisuudella. Viestiaseman periaatekuva tehonsyöttöjärjestelmistä on esitetty kuvassa 7.



Kuva 7. Viestiaseman tehonsyöttöjärjestelmä (Sähköinfo OY:n www-sivut 2012. Hakupäivä 3.11.2012)

7.2 Viestiaseman sähkönsyötön ratkaisut

Varavoimajärjestelmät ovat välttämättömiä viestiasemilla, jotta vältytään palvelukatkoksilta sähkönsyötön häiriötilanteissa. SFS6000 Standardin mukaan varavoimajärjestelmä on syöttöjärjestelmä, jonka tarkoituksena on varmistaa asennuksen tai sen osan toiminnan jatkuminen muista, kuin henkilöturvallisuuteen liittyvistä syistä normaalin syötön keskeytyessä. (SFS6000 2007, 71)

Yleisesti ottaen voidaan varmennettu tehonsyöttö jakaa kolmeen eri osa-alueeseen:

- tasasuuntaajajärjestelmät
- UPS laitteet
- varavoimakoneet.

7.2.1 Tasasuuntaajajärjestelmä

Viestiaseman tasasuuntaajajärjestelmä koostuu yleensä useammasta rinnan kytketystä tasasuuntaajasta, joilla jakeluverkosta tuleva AC sähkö tasasuunataan DC sähköksi. Tasasuuntaajat ovat yleensä järjestelmän vikaantuvin kohta, joten niiden määrä tulee mitoittaa siten, että vähintään yksi laite on laskennallisesti ylimääräinen. Tasasähkö on yleisesti 48V plus-maadoitettu.

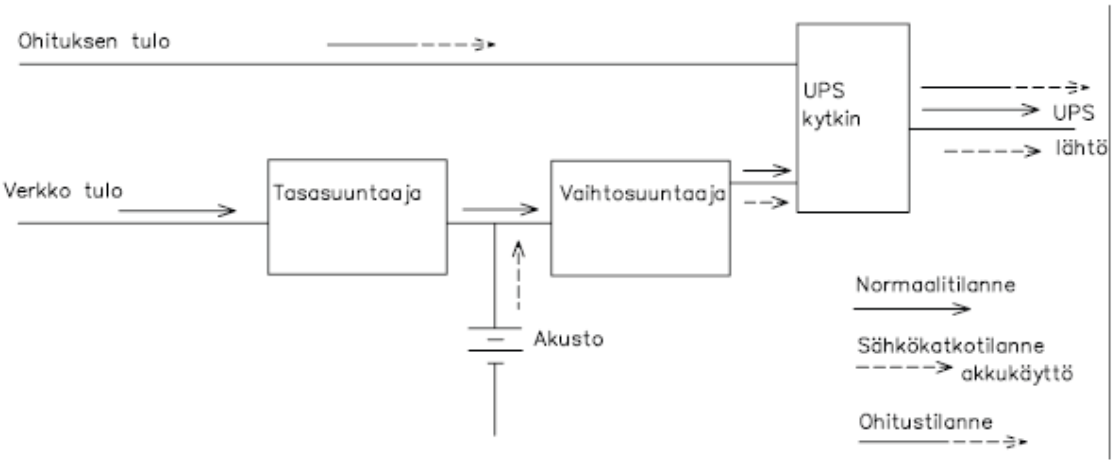
DC sähkö varataan akkuihin, joista sähkö siirretään aktiivilaitteille akuston ja tasasuuntaajajärjestelmän kautta. Akuston koko ja teho mitoitetaan kunkin kohteen DC tarpeen mukaan. Tilat, joihin akut voidaan asentaa, määräytyvät käytössä olevien akkujen tyypin mukaan, ja ilmastoinnin osalta tulee aina noudattaa turvallisuusmääräyksiä. Poikkeusoloihin varautuessa tulee akuston kunnon seurantaan ja huoltoon kiinnittää erityistä huomiota, jottei vikaantuneet tai vajaakapasiteettiset akut yllätä toimimattomuudellaan.

7.2.2 UPS-järjestelmä

Yleisesti ottaen, UPS-järjestelmässä jakeluverkon sähkö syötetään suoraan erilaisten suodattimien kautta. Samalla ladataan järjestelmässä olevia akkuja, ja vikatilanteessa siirrytään syöttämään järjestelmiä akuston ja invertterin kautta. Tässä tutkitaan tarkemmin On-Line UPS-järjestelmää, joka soveltuu parhaiten kriittisten järjestelmien varmistamiseen. Järjestelmässä verkkojännite tasasuunnataan ja taas vaihtosuunnataan invertterillä.

Järjestelmän peruskytkentä on esitetty kuvassa 8. Tämä järjestelmä tuottaa myös laitetilaan mahdolliset DC-syötöt. Järjestelmä suodattaa hyvin verkon jännitteen vaihtelun sekä mahdolliset häiriöt, joten kuormassa ei näy ollenkaan sähkökatkosta järjestelmän siirtyessä akkukäytölle. Mahdollisessa tasasuuntaajajärjestelmässä esiintyvän vian aika-

na järjestelmä siirtyy automaattisesti ohitustilanteeseen, jolloin tasasuuntaaja ja vaihtosuuntaaja ohitetaan



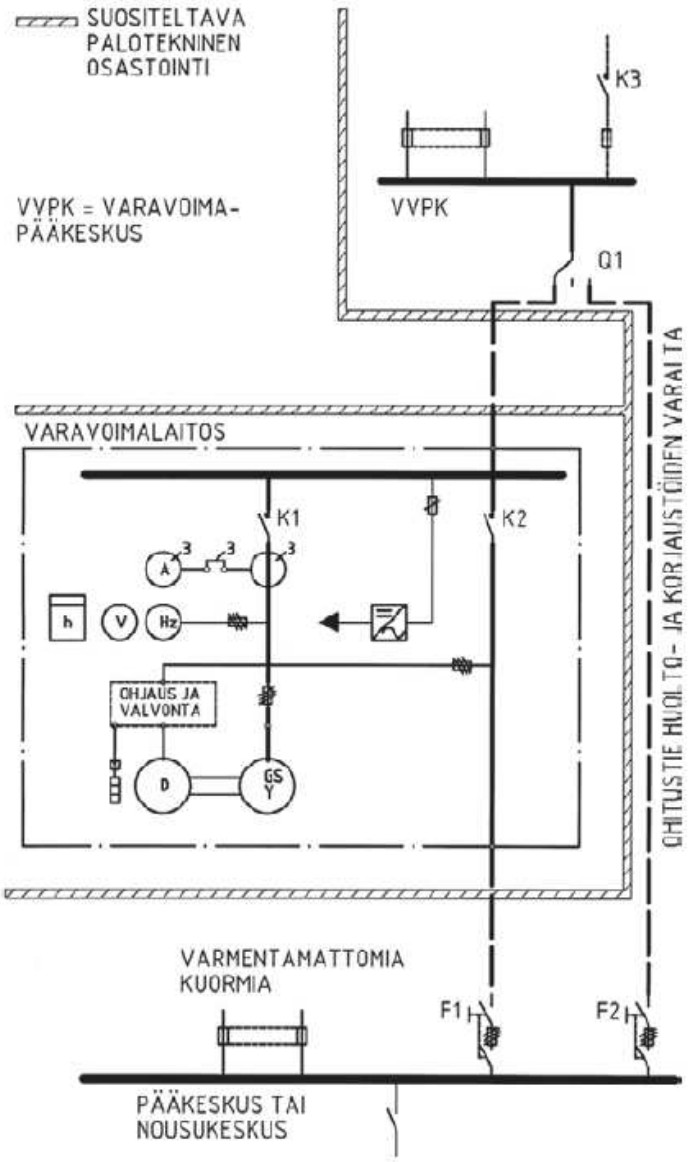
Kuva 8. On-Line UPS periaatekuva (Sähköinfo OY:n www-sivut 2012. Hakupäivä 3.11.2012)

7.2.3 Varavoimakoneet

Kuvassa 9 on esitetty pienen varavoimalaitoksen toimintaperiaate, jossa verkkojännitteen ollessa normaali, VVPK saa syöttönsä katkaisijan K2 kautta. Verkkojännitteen katkettua tai aletessa raja-arvon alle varavoimalaitos käynnistyy, K2 avautuu ja K1 sulkeutuu. Katkoksen pituus riippuu laitoksen tyypistä, normaalisti 5-10s. Verkkojännitteen palautuessa normaaliksi, tapahtuu jälleen syötön vaihto K1 avautuessa ja K2 sulkeutuessa. (Sähköinfo OY:n www-sivut 2012. Hakupäivä 3.11.2012).

Varavoimakoneet on sijoitettava omaan palo-osastoon samoin, kuin niiden tarvitsema polttoaine. Polttoaineen laatua on seurattava säännöllisesti mahdollisen kosteuden syntymisen estämiseksi. Laitteistoa tulee myös koekäyttää ja huoltaa säännöllisesti automaattisen toiminnan varmistamiseksi. Varavoiman on riitettävä teholtaan kaikille IT-laitetilassa sähköä käyttäville laitteistoille, ilmanvaihdolle, jäähdytykselle sekä valaisuun. (Valtionhallinnon tietoturvallisuuden johtoryhmä 2002, 14).

Mikäli varavoimakonetta ei ole ja kohde varustetaan ulkoisen varavoiman syöttömahdollisuudella, tulee syöttöpaikka olla käytettävissä kaikissa tilanteissa. Ulkoiselle varavoimakoneelle tulee olla suunniteltu turvallinen ja sopiva tila, johon kone tai laitteisto voidaan sijoittaa siten, ettei se aiheuta häiriöitä viestiaseman toiminnalle. Ulkoisen varavoimakoneen polttoainehuoltoon tulee kiinnittää erityinen huomio, jotta se voidaan toteuttaa paloturvallisesti.



Kuva 9. Pienen varavoimalaitoksen toimintaperiaate (Sähköinfo OY:n www-sivut 2012. Hakupäivä 3.11.2012)

7.3 Kohteeseen pääsy ja etäisyys huoltohenkilöstöstä

Laitejärjestelmien sijainti maantieteellisesti verrattuna huoltohenkilöstön toimipisteiden etäisyyteen sekä tieverkoston ominaisuudet, vaikuttaa oleellisesti siihen, kuinka nopeasti ongelmatilanteissa saadaan huoltohenkilöstöstä paikalle tekemään korjaus ja ylläpitotehtäviä.

Pohjois-Suomessa viestiasema sijaitsee usein pienten ja hankalasti kuljettavien teiden varrella tai päässä, jolloin keliolosuhteet ja vuodenajat vaikuttavat merkittävästi teiden käytettävyyteen. Tällöin joudutaan usein turvautumaan moottorikelkkoihin ja maastoajoneuvoihin. Erikoistapauksia varten kunnossapidon ja talviaukipidon osalta tulee tehdä tarvittavat ylläpitosopimukset erikseen mahdollisten urakoitsijoiden tai tiehoitokuntien kanssa. Näissä sopimuksissa tulee selvästi kuvata prosessi, yhteystiedot ja vasteajat kuinka kunnossapito toteutetaan.

Pitkien etäisyyksien johdosta alueellisilla toimipisteillä tulisi olla mahdollisimman kattava varaosavarasto erilaisille järjestelmille. Tämä kuitenkaan ei ole aina mahdollista yksittäisten varaosien kustannuksien vuoksi.

7.4 Tiedonsiirtoyhteydet

Tiedonsiirtojärjestelmien oleellinen osa on laitteita yhdistävä tiedonsiirtoyhteys. Yleisesti ottaen yhteydet voidaan jakaa kahteen osaan: langattomat yhteydet ja kaapeliyhteydet. Yhteyden toteutustapa vaikuttaa suuresti siihen, kuinka luotettava ja kestävä se on.

Langattomat yhteydet voidaan jakaa suunta-antenneilla toteutettuihin radiolinkkeihin ja ympärisäteileviin dataradioihin. Kaapeliyhteydet voidaan jakaa kuparikaapeleihin ja valokaapeleihin.

7.4.1 Radiolinkit

Nykyaikaiset digitaaliset radiolinkit ovat suurikapasiteettisia noin STM 4 kapasiteetin omaavia linkkejä. Yleisesti radiolinkkejä pyritään mahdollisuuksien mukaan käyttämään varayhteyksinä, mutta usein ne toimivat myös pääväylinä. Radiolinkkijärjestelmä koostuu yleisesti seuraavista kokonaisuuksista:

- linkkipeili ja säteilijä
- ulkoyksikkö
- sisäyksikkö.

Linkkipeili sijoitetaan yleensä mastoon, jonka korkeus vaihtelee maaston korkeuden ja yhteyden pituuden mukaan. Peilit altistuvat ulkoisten sääolosuhteiden vaikutuksille monin eri tavoin. Voimakkaat tuulet ja myrskyt saattavat rikkoa peilien kiinnikkeet ja kääntää peilin suuntaa, jolloin yhteydet katkeavat. Lumikuormat ja mahdollisesti putoavat jäät saattavat myös rikkoa peilin ja muut rakenteet. Yleisesti talviaikaan mastoon on erittäin vaikea päästä korjaamaan vioittuneita laitteita, koska mastot ovat jäässä. Tämän vuoksi tuleekin pyrkiä suojaamaan mastossa olevat laitteet mahdollisimman hyvin lumi ja jääkuormien vaikutukselta erilaisilla jäänsuojaratkaisuilla. Jos mastossa joudutaan työskentelemään, tulee noudattaa henkilöturvallisuudessa mastotyöskentelyyn liittyviä määräyksiä ja ohjeita, sekä erityistä varovaisuutta.

Antennimastot on suojattava fyysisesti luvatonta kiipeilyä ja ilkivaltaa vastaan, sekä on huomioitava myös ulkopuolisille mahdollisesti aihetuvat vaaratilanteet, kuten mastosta putoava jää. Suojaamista voidaan toteuttaa erilasin aitaratkaisuin, varoituskyltein ja valvontalaitteiden avulla.

7.4.2 Kaapeliyhteydet

Kaapeliyhteydet voidaan jakaa kuparikaapeleihin ja valokaapeleihin, sekä asennustavan mukaan ilma- ja maakaapeleihin. Tässä perehdytään ainoastaan valokaapeleihin, koska tämän päivän runkoyhteydet joudutaan tekemään suurien tiedonsiirtokapasiteettien vuoksi valokaapeleilla. Tällä hetkellä valokaapeliyhteyksillä päästään jopa useiden satojen kilometrien pituuksiin ilman, että välillä tarvitaan vahvistinpisteitä, riippuen kaapeliin asennettavista laitteista. Tämän vuoksi valokaapelin kunnolle asetetaan erittäin suuria vaatimuksia.

Tiedonsiirtoverkossa runkoyhteydet pyritään asentamaan aina maahan ja vain erityistilanteissa käytetään ilmajohtoja. Ilmajohdot ovat erityisen herkkiä vioittumaan esimerkiksi myrskyissä. Mikäli ilmakaapeli asennetaan yhdessä sähköyhtiöiden pylväisiin, on myrskyjen aiheuttamat raivaustyöt turvallisuussyistä sähköyhtiön vastuulla.

Maakaapelit voivat vioittua roudan aiheuttamien ongelmien vuoksi tai muista luonnonolosuhteista, kuten salaman aiheuttamista vioista. Yleisin syy kaapelien vaurioitumiseen on kuitenkin kaivinkoneiden aiheuttamat vioittumiset. Ilkivallan ehkäisemiseksi maastossa olevien kaapelijakamoiden turvallisuuteen tulee myös kiinnittää erityistä huomiota. Jakamoiden määrä tulee pyrkiä pitämään mahdollisimman vähäisenä ja varsinkin taajamien osalta suunnitella hyvin, minne jakamot asetetaan. Jakamot tulee olla aina lukittuina ja avainhallinta jakamoille tulee olla dokumentoituna.

Jo kaapelireittien asennussuunnitteluvaiheessa tulee kiinnittää erityinen huomio ennakoivaan suunnitteluun, jotta tulevaisuudessa kaapeleita jouduttaisiin siirtämään mahdollisimman vähän. Samalla tulisi pyrkiä yhteistyöhön eri operaattoreiden kanssa, jotta pystyttäisiin asentamaan samanaikaisesti useampia kaapeleita

Valokaapelivaipassa olevien kuitujen määrä on kasvanut huomattavasti, esimerkiksi kymmenen vuotta sitten rakennettiin 24 kuituisia kaapeleita ja nykyään 192 kuitua oleva kaapeli on teleoperaattoreilla jo hyvin yleinen runkoverkon kaapeli. Tällaisen kaapelin asentaminen ja korjaaminen vaatii asentajilta erittäin suurta ammattitaitoa ja huolellisuutta. Poikkeusoloissa olosuhteet vaikeuttavat toimintaa ja mahdolliset korjausajat voivat kasvaa huomattavasti. Tämän vuoksi asennus- ja huoltohenkilöstön koulutuksella ja osaamisella on organisaation kannalta suuri merkitys valokaapelijärjestelmien toimivuuden osalta. Poikkeusoloja varten tulisi organisaatiolla olla omia hitsauskykyisiä henkilöitä riittävästi, tai mahdolliset kaapeleiden korjaus- ja ylläpitosopimukset tulee olla ajan tasalla. Samalla tulisi varmistaa, että ulkoistettua palvelua tuottava yritys pystyy todella suoriutumaan tehtävästään. Tämän päivän erilaiset kaapelien rakentamis- ja ylläpitoyritykset tekevät yrityksen rationalisointia ja tällöin saatetaan osa osaavaa kaapelien korjaushenkilöstöä irtisanoa.

Puolustusvoimilla ei ole ainoastaan omaa kaapeliverkkoa, vaan osa kaapeleista on hankittu erilaisilla sopimuksilla toiselta osapuolelta. Hankituista kaapeleista tulee saada

dokumentaatio mahdollisimman tarkasti, jotta pystytään tekemään ennakkosuunnitelmaa mahdollisia poikkeusoloja varten. Yhteistyösopimuksissa sovitaan, kuinka organisaatioiden käyttökeskukset pitävät yhteyttä toisiinsa erilaisissa vika- ja muutostilanteissa.

7.5 Kohteen fyysinen turvallisuus

Tilaturvallisuuden tarkoituksena on osana fyysistä turvallisuutta suojata henkilöstöä, tietoa ja materiaalia. Tilaturvallisuudella tarkoitetaan kaikkia niitä rakenteellisia ja valvonnallisia järjestelyjä, joilla varmistetaan tilojen pysyminen vain oikeutettujen hallinnassa ja käytössä sekä käyttötarkoituksen edellyttämässä kunnossa. Rakenteilla tarkoitetaan seiniä, kattoja, ikkunoita, ovia, paloturva- ja kassakaappeja sekä muita mekaanisia ratkaisuja. Valvontajärjestelmillä tarkoitetaan yleensä kulunvalvonta-, tunkeutumisen ilmaisu-, kameravalvonta- ja olosuhdevaroitusjärjestelmiä. Sähköisiin valvontajärjestelmiin kuuluvat myös kiinteistöautomaatiojärjestelmät, joilla valvotaan ja ohjataan tilan käyttöolosuhteita. Tilaturvallisuuden kokonaisuudesta ei ole olemassa varsinaisia standardeja, mutta kunkin tietoturvallisuustason mukaiset viranomaisvaatimukset on esitetty yksityiskohtaisesti Kansallisen turvallisuusauditointikriteeristön (KATAKRI) fyysisen turvallisuuden osiossa. Viestiasemien sijainnin suunnittelulla on tärkeä osa kokonaisturvallisuuden kannalta.

Viranomaisen on määriteltävä vastuullaan olevien tilojen turvallisuusratkaisut. Määrittelyssä on huomioitava mm. rakenteelliset ratkaisut, tarvittavat valvontajärjestelmät ja mahdollisesti tilojen käyttöoikeuksiin liittyviä asioita. Tilaturvallisuutta tulee tarkastella kokonaisuutena. Kokonaisuuteen kuuluvat esim. tietoverkkojen laite- ja ristikytkentätilojen tilaturvallisuuden huomioiminen sekä huolehtiminen siitä, etteivät asiattomat pääse käsiksi mm. aktiivisiin kytkentärasioihin.

Valvontajärjestelmillä valvotaan kulkua tiloihin ja havaitaan asiaton liikkuminen niissä. Valvontajärjestelmät ovat tietojärjestelmiä ja ne tuottavat usein henkilörekistereitä. Kameravalvonnassa työpaikalla ja viestiasemilla on noudatettava, mitä laissa yksityisyyden suojasta työelämässä (759/2004) säädetään.

Valvontajärjestelmien tietoturvallisuudesta tulee huolehtia vastaavalla tavalla kuin huolehditaan muidenkin tietojärjestelmien tietoturvallisuudesta. Kiinteistöautomaatiojärjestelmien tietoturvallisuuden tulee olla asianmukaista ja erityisesti käyttöoikeuksien hallinnan on oltava valvottua.

Kiinteistöautomaatiojärjestelmillä huolehditaan laitetilojen käyttöolosuhteista ja niihin vaikuttamalla voidaan tietojärjestelmien palvelut romahduttaa. Kiinteistöautomaatiojärjestelmiä voidaan usein etävalvoa, jolloin olosuhteiden muuttaminen voi tapahtua viranomaisen ulottumattomista.

Tilaturvallisuudessa on otettava huomioon myös tilojen äänieristys. Äänieristys on huomioitava kaikissa niissä tiloissa, joissa käsitellään salassa pidettävää tietoa. Erityistä huomiota on kiinnitettävä kaapelien läpivienteihin ja ilmanvaihtojärjestelmän kautta kulkevan äänen eristämiseen. Sähkömagneettisesta hajasäteilystä syntyvä uhka on huomioitava erikseen määriteltävissä tapauksissa toimivaltaisen viranomaisen määrittämässä laajuudessa (Tempest-suojaukset). (Valtionhallinnon tietoturvallisuuden johtoryhmä 2002, 14).

7.6 Sidosryhmäturvallisuus

Yhteistoimintaa sidosryhmien kanssa säätelee kansallinen lainsäädäntö. Muun muassa perustuslaki, julkisuuslaki, henkilötietolaki ja sähköisen viestinnän tietosuojalaki sekä tietoturvallisuusasetus asettavat vaatimuksia, jotka on otettava huomioon käytettäessä ulkopuolisia organisaatioita osana viranomaistehtävien hoitamista. Tällaisia ovat esimerkiksi tietosuojaan ja varautumiseen liittyvät sijaintirajoitteet.

Tietoteknisten järjestelmien ja palvelujen kehittämiseen ja ylläpitoon liittyy useilla viranomaisilla turvallisuusluokiteltavan tietovarannon käsittelytehtäviä. Tästä syystä toimeksiannot tulee suunnitella etukäteen huolella, ja varmistua toimittajien kyvystä suojata heidän käyttöönsä annettavaa luokiteltua tietovarantoa. Toimeksiannot tulisi tehdä sellaisten yritysten kanssa, joilla on Suomessa riittävän vahvat toiminnot ja tuki toimeksiannon kannalta.

Mikäli hankintaan tai palveluun liittyy luokiteltavan tietovarannon käsittelyä, tulee toimittajan kanssa varmistua etukäteen turvallisuusjärjestelyistä. Mikäli kyse on ulkomaisista toimijoista ja henkilöistä, tulee kääntyä kansallisen turvallisuusviranomaisen puoleen ja pyytää tätä selvittämään kyseisen toimijan ja henkilöstön osalta tarvittavat turvallisuustiedot. (Valtionhallinnon tietoturvallisuuden johtoryhmä 2002, 18).

7.7 EMP suojaus

Termillä EMP (ElectroMagnetic Pulse) tarkoitetaan useimmiten ydinräjähdyksessä syntyvää sähkömagneettista pulssia, mutta syntymekanismi voi olla muukin. On määritelty muutamia tarkentavia alakäsitteitä. Termiä NEMP (Nuclear Electro-Magnetic Pulse) käytetään, kun halutaan painottaa, että pulssi on tuotettu erityisesti ydinräjähdyksellä. Kaikissa ydinräjähdyksissä syntyy aina jonkinasteinen sähkömagneettinen pulssi. Tietyissä erikoistilanteissa pulssi voi olla hyvinkin voimakas, kuten esimerkiksi korkealla ilmakehän yläpuolella tapahtuvassa ydinräjähdyksessä. Tällöin pulssista käytetään nimitystä HEMP (High altitude ElectroMagneticPulse). Muutkin ilmiöt kuin ydinräjähdykset voivat tuottaa sähkömagneettisen pulssin. Esimerkiksi salaman iskussa syntyvää pulssia kutsutaan nimellä LEMP (Lightning ElectroMagnetic Pulse). LEMP on voimakkuudeltaan huomattavasti esimerkiksi HEMP pulssia heikompi, mutta voi silti olla merkittävä pienillä etäisyyksillä. (Puolustusvoimien www-sivut 2012. Hakupäivä 3.1.2012).

EMP:ltä voidaan suojautua käytännössä kahdella eri tavalla, käyttäen joko fyysistä suojausta tai parantamalla laitteiden häiriönkestoisuutta. Fyysisessä suojauksessa rakennetaan teräspellistä erillisiä laitekaappeja tai kokonaisia huoneita joihin herkät laitteistot asennetaan. Laitevalmistajat ovat alkaneet myös valmistamaan laitteita, jotka ovat EMP kestäviä, jolloin niiden osalta suojaustoiminnat kohdennetaan lähinnä häiriösietoisuuden parantamiseen. Häiriösietoisuutta parantaessa kiinnitetään huomioita esimerkiksi kaapelointiin, missä valokaapelilla saadaan tuotettua häiriöttömiä yhteyksiä koska se ei johda sähkömagneettisia aaltoja.

EMP suojauksen teoria ja rakennustekniikka on laaja kokonaisuus, joista on saatavissa useita tieteellisiä julkaisuja. Kuvassa 10 on esitetty järjestelmäkaappi, joka suojaa sisälle asennettavia laitteita EMP vaikutuksilta. Kaappi koostuu teräksisestä suojakuoresta,

jossa riittävän suojauksen saavuttamiseksi kaapeloinnit ja ilmastointi on hoidettu erilaisilla suotimilla ja läpivienneillä.

Kuva 10. Järjestelmäkaappi (Fitelnetin www-sivut 2012. Hakupäivä 30.10.2012)

EMP suojarakentaminen on erikoisosaamista vaativaa työtä, joka edellyttää erityisiä materiaaleja, komponentteja sekä mittalaitteita suojaustason saavuttamisen toteuttamiseksi. Rakennetuille kohteille tuleekin tehdä vaatimustenmukaiset mittaukset joko oman henkilöstön tai ulkopuolisen tahon toimesta mahdollisimman pian kohteen valmistumisen jälkeen. EMP tilojen ylläpitäminen vaatikin erityistä huolellisuutta ja tarkkuutta kaikilta käyttäjiltä, jotta suojaustaso ei heikennetä mahdollisesti väärillä asennuksilla ja laitejärjestelmillä.

8 YHTEENVETO

Työn tavoitteena oli tutkia poikkeusolojen kannalta PSJJK:n ylläpidossa olevien tiedonsiirtojärjestelmien mahdollisia kriittisiä kohteita ja selvittää sitä, ovatko niiden vaikutukset samantyyppisiä niin normaalioloissa, kuin mahdollisissa poikkeustilanteissa. Työssä kehitetyllä riskianalyysimallilla voidaan viestiasemat laittaa kriittisyyden perusteella haluttuun järjestykseen. Henkilöstölle suunnitellulla koulutuskartoituksella voidaan saada tarkempaa tietoa ylläpitohenkilöstön osaamisesta ja riittävyydestä. Tässä työssä ei kuitenkaan tehty kartoituskyselyä, vaan se toteutetaan mahdollisesti myöhemmässä vaiheessa.

Kriittisimpänä kohteena tutkimuksen aikaan selvisi, että sähköenergian saatavuus on tärkein tekijä tiedonsiirtoverkkojen ja niillä toimitettavien palveluiden osalta. Energian saanti tulisikin saada turvattua kaikissa olosuhteissa, ja näin ollen pitää kehittää keinoja, joilla mahdollisia sähkökatkoja voidaan sietää paremmin.

Riskianalyysin tekeminen on haastavaa, koska tietoa täytyy saada usealta eri taholta, jotta voidaan todeta riskin laatu. Tietoja joudutaan hankkimaan ja selvittämään niin kiinteistöjen omistajilta, kuin sähköyhtiöiltä, teleoperaattoreilta ja useilta yhteistyökumppaneilta. Tavoitteena olikin laatia yksi esimerkki määrittelytavasta ja tarkistuslistasta, jolla puolustusvoimat tai teleoperaattori voi selvittää omia kriittisiä kohteita, ja näin ollen kehittää omaa toimintaansa. Jokainen toimiala voikin omassa toiminnassaan miettiä omalta osaltaan niitä kohteita joita omaan tutkimukseensa ottaa.

LÄHTEET

Aalto, Heikki, 1994. Kunnossapitotekniikan perusteet. Helsinki: Kunnossapitoyhdistys ry.

Energiateollisuuden www-sivut 2011. Hakupäivä 4.5.2012.<http://www. energia.fi>

Fitelnetin www-sivut 2012. Hakupäivä 30.10.2012. <http://www.fitelnet.fi>

Ilmonen, Ilkka & Kallio, Jani & Koskinen, Jani & Rajamäki, Markku 2010. Johda Riskejä. Helsinki: Tammi.

Järviö, Jorma 2004. Kunnossapito. Helsinki: KP-Media Oy.

Malmi, Teemu & Peltola, Jukka & Toivanen, Jouko 2006. BALANCED SCORCARD Rakenna ja sovella tehokkaasti. Helsinki: Talentum.

Mäkinen, Kalevi 2007. Organisaation strateginen kokonaisturvallisuus. Helsinki: Edita.

Otala, Leenamaija 2008. Osaamispääoman johtamisesta kilpailuetu. Helsinki: Wsoy.

Otala, Leenamaija & Pöysti, Kaija 2012. Kilpailukyky 2.0 kilpailukykyhyppy yhteisöllisillä toimintatavoilla. Helsinki: Helsingin Kamari Oy.

PK-RH www-sivut 2012. Hakupäivä 13.10.2012. <http://www.pk-rh.com>

Puolustusvoimien www-sivut 2012. Hakupäivä 3.1.2012. <http://www.puolustusvoimat.fi>

PSK 6201, 2009. Kunnossapito käsitteet ja määritelmät, 3 painos. Helsinki: PSK standardisointi.

Salmela, Hannu & Hallanoro, Mikko & Sippa, Seppo & Tapaninen, Tommi & Ylitalo, Jari 2010. Ketterän Organisaation IT. Helsinki: Talentum.

SFS-EN 13306, 2010. Kunnossapidon terminologia, 2. painos. Helsinki: SFS.

SFS-käsikirja 6000, 2007. Pienjänniteasennukset 1. painos. Helsinki: SFS.

Sähköinfo OY:n www-sivut 2012. Hakupäivä 3.11.2012. <http://www. sahkoinfo.fi>

Valtionhallinnon tietoturvallisuuden johtoryhmä, 2002. Tietoteknisten laitetilojen turvallisuussuositus VAHTI 1/2002. Helsinki: Valtionvarainministeriö.

Valmiuslaki 29.12.2011/1552.

Valtionvarainministeriön www-sivut 2012. Hakupäivä 30.11.2011. <http://www.vm.fi>

Viestintämarkkinalaki 23.5.2003/393.

LIITEET

Liite 1. Riskikartoitus

Liite 2. Osaamiskartoitus

RISKIANALYYSI

KOHDE: _____

LAATIJA: _____

LAADITTU: _____

Riskilaji	**Riski, kuvaus**	**Todnäk**	**Vaikutus**	**Riski**
INFRA	Laitetilan omistus, onko oma laitetila	1	2	2
	Laitetilan omistus vaikuttaa siihen pääseekö ulkopuolisia henkilöitä tilaan: omatila vieraan tilassa, vieraan laitteita meidän tilassa, laitteet vieraassa tilassa			
INFRA	Laitetila sijainti ja pääsy	2	5	10
	Laitetilan sijainti vaikeakulkuisessa maastossa: taajama, maaseutu, talvella ei aurattu, tunturimaasto			
INFRA	Sähköinen suojaus	2	3	6
	Ylijännitesuojat, maadoitukset			
INFRA	EMP suojaus	1	5	5
	EMP suojauksen taso: HPM=1, EMP=3, Ei suojausta=5			
INFRA	Ilmastointilaitteen ikä ja omistus	2	3	6
	Ikä alle 1vuosi ja oma=1, ikä alle 3vuotta ja oma =2, ikä alle 5 vuotta ja oma =3, ikä yli 5vuotta ja oma =4, Ei ilmastointia=5, Ikä alle 1vuosi ja vieras=2, ikä alle 3vuotta ja vieras =3, ikä alle 5 vuotta ja vieras =4, ikä yli 5 vuotta ja vieras =4			
INFRA	Tulipalon mahdollisuuden rajoittaminen	1	2	2
	Onko pakkausmateriaaleja ja muuta turhaa aineistoa kohteessa			
INFRA	Sammutusjärjestelmä	2	4	8
	Sammutusjärjestelmän olemassaolo ja ikä			
INFRA	Kulunvalvonta	1	2	2
	Henkilöstön kulkuoikeudet			
INFRA	Rikosilmoitusjärjestelmä	1	4	4
	Hälytysten siirto, prosessi			
INFRA	Sähkönsyötön kahdennus	1	3	3
	Onko kohteessa erilliset sähkönsyötöt			

INFRA	Vesivahinko	1	3	3
	Kulkeeko kohteen kautta vesijohtoja, viemäreitä			
INFRA	Akuston ikä	1	3	3
	<1v=1;1- 2v=2; 3-5=3; 6-7=3; >7=5			
INFRA	Tasasuuntaajien ikä	1	3	3
	<1v=1;1- 2v=2; 3-5=3; 6-7=3; >7=4			
INFRA	Varavoimakone, ikä	1	3	3
	<1v=1;1- 2v=2; 3-5=3; 6-7=3; >7=4			
INFRA	Polttoainesäiliö	1	3	3
	tilavuus 500l, 1000l, 2000l, >2000l			
INFRA	Sähköt maassa, ilmassa	1	3	3
	Ilmakaapelit aiheuttavat lisäriskin sähkönsyöttöön			
Tietoliik	Varaosatilanne	1	3	3
	Mikä on laitteiden varaosatilanne saatavilla			
Tietoliik	Dokumentaatio	1	3	3
	Onko dokumentaatio olemassa			
Tietoliik	Runkoyhteyden sijainti	1	3	3
	Ilmakaapeli, maakaapeli			
Tietoliik	Runkoyhteyksien toteutus	1	3	3
	Ovatko yhteydet kaapelilaitteilla vai linkeillä			
Tietoliik	Hallintatyökalujen olemassaolo	1	3	3
	Onko paikallista kykyä hallita laitteita			
Tietoliik	Runkoyhteyksien kahdennus	1	3	3
	Onko runkoyhteydet kahdennettu			
Tietoliik	Jakamoita kohteessa ulkona	1	2	2
	Jakamot ovat mahdollisia ilkivalta kohteita			
Tietoliik	Runko kapasiteetti	1	3	3
	STM 1,4, 16, CWDM, DWDM			
Tietoliik	Palveltavat asiakkaat kohteessa	1	3	3
	Tärkeys normi käyttäjä =3, johto=4, viranomaiset =5			
HENK	Oman henkilön etäisyys kohteesta	1	3	3
	<10 km=1; 10-100=2; >100=3			
HENK	Ulkoistetun henkilöstön etäisyys	1	3	3
	<10 km=1; 10-100=2; >100=3			
HENK	Osaamistaso/riittävyys	1	3	3
	Henkilöstö määrä ja osaaminen			
HENK	Yhteydenpitovälineet	1	3	3
	VIRVE, GSM, ei välineitä			
HENK	Onko ulkoistetut palvelut sovittu	1	3	3
	Ylläpitosopimukset: Ilmastointi, Kaapelit, Sähköt			

Vaikuttavuuden määrittely

1	Vähäinen vaikutus toimintakykyyn, hetkelliset toimintahäiriöt, ei toiminnan keskeytymistä.
2	Pieni vaikutus toimintakykyyn, toiminta häiriintyy osittain, lyhyt toiminnan keskeytyminen.
3	Kohtalainen vaikutus toimintakykyyn, toiminta häiriintyy laajamittaisesti, toiminta keskeytyy määräajaksi.
4	Suuri vaikutus toimintakykyyn, toiminta lakkaa toistaiseksi.
5	Katastrofaalinen vaikutus toimintakykyyn, toiminta lakkaa kokonaan, huomattavan suuri ja pitkälle tulevaisuuteen ulottuvia vaikutuksia.

Todennäköisyyden määrittely

1	Erittäin harvinainen riski, korkeintaan kerran 50 vuodessa
2	Harvinainen riski, kerran 25 vuodessa
3	Melko harvinainen riski, kerran 10 vuodessa
4	Melko todennäköinen riski, kerran vuodessa
5	Erittäin todennäköinen riski, useita kertoja vuodessa

Riskiluku

Riskiarvio	Uhka toiminnan jatkuvuudelle
< 10	Vähäinen riski
10-20	Kohtalainen riski
> 20	Merkittävä riski
kaava	Riski = todennäköisyys x vakavuus, (arvot, välillä 1-5)

Työssäoppiminen ja koulutusten toimivuus

Yrityksen työntekijöiden kehittäminen ja osaamisen kartoitus

Taustatiedot

Nimi_____ **Tehtävä**_____

Ikä

- ☐ Alle 20 vuotta
- ☐ 20-30 vuotta
- ☐ 31-40 vuotta
- ☐ 41-50 vuotta
- ☐ 51-60 vuotta
- ☐ yli 60 vuotta

Nykyinen työsuhteen kesto

- ☐ alle 6kk
- ☐ 6kk-12kk
- ☐ 1-2 vuotta
- ☐ 2-5 vuotta
- ☐ 5-10 vuotta
- ☐ yli 10 vuotta

Eläkkeelle jäämiseen aikaa

- ☐ Alle 5 vuotta
- ☐ 6-10 vuotta
- ☐ yli 11 vuotta

Aikaisempi kokemus alalta

- ☐ ei aikaisempaa kokemusta
- ☐ alle 1 vuosi
- ☐ 1-2 vuotta
- ☐ 2-5 vuotta
- ☐ yli 5 vuotta

Työsopimus

- ☐ osa-aikainen
- ☐ työsopimussuhteinen
- ☐ virkasuhteinen

Toimitko esimies asemassa

- ☐ kyllä
- ☐ ei

Mitkä asiat koet tärkeäksi työssäoppimisessa

1= Täysin eri mieltä, 2=Osittain eri mieltä, 3=Osittain samaa mieltä, 4= Täysin samaa mieltä	1	2	3	4
Työn tekeminen on merkittävää työssäoppimisen kannalta				
Sosiaalinen vuorovaikutus työkavereiden kanssa on tärkeä työssäoppimisen keino				
Sosiaalinen vuorovaikutus asiakkaiden kanssa on tärkeä työssäoppimisen keino				
Sosiaalinen vuorovaikutus yhteistyökumppaneiden kanssa on tärkeä työssäoppimisen keino				
Esimiehen palaute on oleellista työssäoppimisessa				
Kehityskeskustelu esimiehen kanssa on oleellista työssäoppimisessa				
Tuotekoulutus on tärkeä osa työssäoppimista				
Henkilöstökoulutus on tärkeä osa työssäoppimista				
Omatoiminen ammatillinen pätevöityminen on tärkeä osa työssäoppimista				
Yrityksen kirjallisten-, sekä verkkomateriaalinen hyödyntäminen on merkittävää työssäoppimisen kannalta				

Ota kantaa seuraaviin työyksikköäsi toimintaa koskeviin väittämiin

1= Täysin eri mieltä, 2=Osittain eri mieltä, 3=Osittain samaa mieltä, 4= Täysin samaa mieltä	1	2	3	4
Olen saanut riittävän perehdytyksen nykyisiin työtehtäviini				
Sisäinen opiskelumateriaali on onnistunut				
Työyksikkö on onnistunut henkilöstö koulutuksessaan				
Saan tarvittaessa apua työkavereiltani				
Työyksikön keskeiset tavoitteet ovat selkeitä				
Olen saanut palautetta työstäni viimeisen 12kk aikana				
Työyksikössä on motivoiva ilmapiiri				

Mitkä yrityksen koulutusmetodit olet kokenut hyväksi työsi kannalta

1= Täysin eri mieltä, 2=Osittain eri mieltä, 3=Osittain samaa mieltä, 4= Täysin samaa mieltä	1	2	3	4
Työyksikön perehdytys on auttanut minua työssäni				
Laitevalmistajien koulutukset ovat olleet hyödyllisiä työssäni				
Oman organisaation koulutukset ovat olleet hyödyllisiä työssäni				
Sidosryhmien(tavarantoimittajat) koulutukset ovat olleet hyödyllisiä työssäni				

Turvallisuuteen ja ajamiseen liittyviä lupia

- [ ] Mastotyökortti
- [ ] Sähköasennus oikeudet. Mikä?
- [ ] E- ajokortti
- [ ] C-ajokortti
- [ ] telakuorma-auto kortti
- [ ] moottorikelkkakortti
- [ ] tulityökortti
- [ ] sähkötyöturvallisuuskortti
- [ ] EA 1 / EA 2
- [ ] Tieturvallisuuskortti
- [ ] Muu mikä?

Kuinka hyvin mielestäsi osaat seuraavat järjestelmät

1= Tunnistamistasa, 2= Käyttäjä, 3= Osaaja, 4= Vahva osaaja	**1**	**2**	**3**	**4**
Siirtolaitejärjestelmä1				
Siirtolaitejärjestelmä2				
Siirtolaitejärjestelmä3				
Siirtolaitejärjestelmä4				
Siirtolaitejärjestelmä5				
Siirtolaitejärjestelmä6				
Datajärjestelmä1				
Datajärjestelmä2				
Datajärjestelmä3				
Datajärjestelmä4				
Siirrettävät varavoimakoneet				
Valokaapeli hitsauslaitteet				
Valokaapelitutkan käyttö				
HF-laitteet				
VHF-laitteet				

Vapaa sana: lisää tähän mahdolliset IT-alan sertifikaatit jne